

2-14-00

Atty. Docket No. RSW00-0010

A

jc604 U.S. PTO



02/11/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application Transmittal

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the **Patent Application** of:

Inventor: K. S. Attwood, et al

For: Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol

Enclosed are:



1 sheets of drawings.



An assignment of the invention to International Business Machines Corporation, Armonk, New York 10504.



A certified copy of a _____ application.



An associate power of attorney.



Declaration and Power of Attorney for Patent Application

The filing fee has been calculated as shown below:

(Col. 1)

(Col. 2)

Other Than Small Entity

For:	No. Filed	No. Extra
Basic Fee		
Total Claims	8-20 =	0
Indep. Claims	4-3 =	1
<input type="checkbox"/> Multiple Dependent Claim Presented		

Rate	Fee
	\$690.00
x \$18.00=	\$.00
x \$78.00=	\$78.00
\$260.00	\$.00
Subtotal	\$.00
\$130.00	\$768.00
TOTAL	\$768.00

Surcharge-Late Filing Fee or Oath or Declaration

Deposit Account Authorization



Please charge Deposit Account No. 09-0461 in the amount of \$768.00. A duplicate copy of this sheet is enclosed.



The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 09-0461. A duplicate copy of this sheet is enclosed.



Any additional filing fees required under 37 C.F.R. §1.16.



Any patent application processing fees under 37 C.F.R. §1.17.

Date: February 11, 2000

Respectfully submitted,

By

Jerry W. Herndon
 Jerry W. Herndon
 Attorney of Record
 Registration No. 27,901
 IBM Corporation
 Intellectual Property Law
 Dept. T81/Bldg. 062
 P.O. Box 12195
 Research Triangle Park, NC 27709
 Telephone: 919- 543-3754
 Fax: 919-254-4330

EXPRESS MAIL CERTIFICATE

Express Mail Label Number: EJ922477658US
Date: February 11, 2000

I hereby certify that I am depositing the enclosed or attached paper with the U.S. Postal Service "Express Mail Post Office to Addressee" service on the above date, addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Jennifer Dianne Lane
 Jennifer Dianne Lane

EXPRESS MAIL LABEL NO.: EJ922477658US DATE OF DEPOSIT: 2/11/2000
I hereby certify that this paper and fee are being deposited with the United States Postal Service
Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and
is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Jennifer Dianne Lane Jennifer Dianne Lane
NAME OF PERSON MAILING PAPER AND FEE SIGNATURE OF PERSON MAILING PAPER AND FEE

INVENTORS: K. Attwood, L. Overby, J. Sun

Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol

Technical Field

The invention relates generally to the field of networking and specifically to defending against attacks by malicious users attempting to disable a server by flooding the server with connectionless datagrams.

Background of the Invention

Flooding attacks have recently been used with increasing frequency to target and disable servers on the Internet. A flooding attack occurs when a user sends a large number of

requests to a server in a relatively short period of time with an intent to overload and thereby disable the server. A flood of packets from a malicious user can overload a server in the same way that a flood of packets from a misconfigured system can overload a server. But the end result is the same; the server becomes overloaded in trying to service the requests. This prevents legitimate requests from being timely served and often disables a server or causes it to crash. A number of flooding attacks have been reported in the news recently on some well known web sites. These attacks were characterized by a flood of individual connection requests to establish initial communications. A related patent application, serial number _____ discloses an algorithm to defend against such connection request attacks. However, it is also possible to attack a server by flooding it with connectionless datagrams, such as might occur in the UDP (user datagram) protocol. The effect is essentially the same; the server becomes overloaded in trying to service the horde of datagrams and can even become totally disabled. Flooding attacks are very difficult for traditional intrusion detection systems to prevent due to the difficulty of determining whether the traffic is legitimate or not.

Summary of the Invention

The invention recognizes that the consequences of intentional datagram flooding attacks and unintentional

overload situations resulting from a burst of datagrams can be mitigated by dropping the traditional notion of attempting to distinguish between legitimate and illegitimate traffic. In the invention, all datagram traffic is subject to a policy that attempts to guarantee that legitimate work will be performed and a server will not crash in flooding situations, irrespective of whether the flooding is caused by legitimate or illegitimate datagram traffic. The invention helps to prevent a server from crashing due to overload and it prevents one or more attackers from consuming all server resources.

In response to the arrival of a datagram destined for a specified port on a server, the transmitting host is determined and the number of datagrams already queued for the same host and for the same port is determined. If this number exceeds a first threshold, the request for a connection is denied.

The first threshold is dynamically determined in the preferred embodiment. The owner of a server specifies for each port that is subject to datagram flooding checks a maximum number of queued datagrams (M) allowed at any time to the port and a controlling percentage (P) of available queue slots remaining for the port. The invention keeps track of the number (A) of queued datagrams for the port and it calculates the number of available queue slots (I) by subtracting the number of queued datagrams from the maximum

number of datagrams ($I = M - A$). If the number of datagrams already queued for the transmitting host is equal to or greater than P times the number of queue slots left ($\Rightarrow P \cdot I$), then the present datagram is refused. Otherwise, the datagram is queued and the number of queued datagrams (A) for the port is incremented by one.

The maximum number of datagrams and the threshold percentage P will be difficult for most owners to configure. Therefore, a "statistics" mode is provided that measures normal traffic loads of different servers and suggests an appropriate maximum and threshold that will not hamper similar legitimate traffic loads. This statistics mode is not part of the claimed invention and is not described further herein.

Brief Description of the Drawing

In the drawing:

Fig. 1 shows an illustrative flowchart of operations executed at a server in response to the receipt of a datagram to ensure that a flooding situation does not prevent the completion of other work and does not crash the server.

Detailed Description

The invention requires that an owner of a server that

uses the invention configure the server with certain parameters for use by the invention. By way of example, the preferred embodiment requires that the owner specify for each port number subject to datagram flooding checks a maximum number of datagrams (M) allowed at any time to be queued to the port and a controlling percentage (P) of available queue slots remaining for the port. The percentage P is used to establish a threshold to trigger the denial to service a datagram. As datagrams are queued and serviced, the server dynamically maintains the number of available queue slots for each port that is subject to flooding checks.

An entry is made to step 100 in Fig. 1 when a datagram is received at a network server. The first step 106 determines from the datagram the port number to which the datagram is directed. The port number contained in a datagram represents a destination within a given host computer to which the datagram is to be delivered. Some ports are reserved for standard services. For example, the Network File System (NFS) is one example of a standard service that receives UDP datagrams.

The identity (the IP address) of the sending host is also determined from the datagram. The port number is used by step 108 to locate a memory control block for the port or to create one if a port control block does not presently exist. Attached to the port control block are a plurality of host

control blocks for hosts that presently have one or more datagrams in queue. If the sending host does not have a host control block, one is created. A host control block contains, among other things, a count of the port connections presently assigned to the host.

Step 108 determines from the datagram the identity of the transmitting host that initiated the datagram and it uses the port number and the host identity to locate a memory control block or it creates a memory control block if one does not presently exist. An existing memory control block contains, among other things, a count of the number of datagrams presently queued by the host. Step 108 determines the port number to which this datagram is directed.

At step 110, the server fetches from the memory control block the maximum number of queued datagrams M specified for this port number, the controlling percentage P and the number A of queued datagrams. Step 112 calculates the number I of available queue slots as $M - A$. Step 114 determines if the number of datagrams already queued to the transmitting host is equal to or greater than P times I . If so, then the datagram is discarded and the queuing algorithm exits at 118. On the other hand, if the number of queued datagrams already initiated by the transmitting host is less than P times I , the datagram is queued for service at step 116 and A is incremented by one to update the number of datagrams in queue for this port number.

The computer program that has been described can be executed on virtually any type of computer, ranging from personal computers to large mainframes such as IBM's System 390 machines. The only requirement is that the computer is configured with network communication software and is accessible as a server via a network.

Skilled artisans in the fields to which the invention pertains will recognize that numerous variations can be made to the embodiments disclosed herein and still remain within the spirit and scope of the invention.

What is Claimed:

1 1. A method of preventing a flooding attack on a network
2 server in which a large number of connectionless datagrams are
3 received for queuing to a port number on the server,
4 comprising:

5 determining, in response to the arrival of a datagram
6 from a host for a port number on the server, if the number of
7 datagrams already queued to the port number from the host
8 exceeds a prescribed threshold, and, if so,

9 discarding the datagram.

10 2. The method of claim 1 wherein the determining if the
11 number of datagrams already queued to the port number from the
12 host exceeds a prescribed threshold further comprises:

13 calculating the prescribed threshold by multiplying a
14 percentage P by the number of available queue slots for the
15 port number.

16 3. Apparatus for preventing a flooding attack on a network
17 server in which a large number of datagrams are received for
18 queuing to a port number on the server, comprising:

4 means for determining, in response to a datagram from a
5 host for a port number on the server, if the number of
6 datagrams queued on the port by the host exceeds a prescribed
7 threshold, and

8 means responsive to the determining means for discarding
9 the datagram.

1 4. The method of claim 3 wherein the means for determining
2 if the number of datagrams already queued to the port from the
3 host exceeds a prescribed threshold further comprises:

4 means for calculating the prescribed threshold by
5 multiplying a percentage P by the number of available queue
6 slots for the port number.

7 5. A storage media containing program code segments for
8 preventing a flooding attack on a network server in which a
9 large number of datagrams are received for queuing to a port
number on the server, comprising:

5 a first code segment activated in response to a datagram
6 from a host for a port number on the server for determining if
7 the number of datagrams already queued to the port from the
8 host exceeds a prescribed threshold, and

9 a second code segment responsive to the first code

10 segment for discarding the datagram.

1 6. The storage media of claim 5 wherein the first code
2 segment further comprises:

3 a third code segment for calculating the prescribed
4 threshold by multiplying a percentage P by the number of
5 available queue slots for the port number.

1 7. A carrier wave containing program code segments for
2 preventing a flooding attack on a network server in which a
3 large number of datagrams are received for queuing to a port
4 number on the server, comprising:

5 a first code segment activated in response to a datagram
6 from a host for queuing to a port number on the server for
7 determining if the number of datagrams already queued to the
8 port from the host exceeds a prescribed threshold, and
9

10 a second code segment responsive to the first code
segment for discarding the datagram.

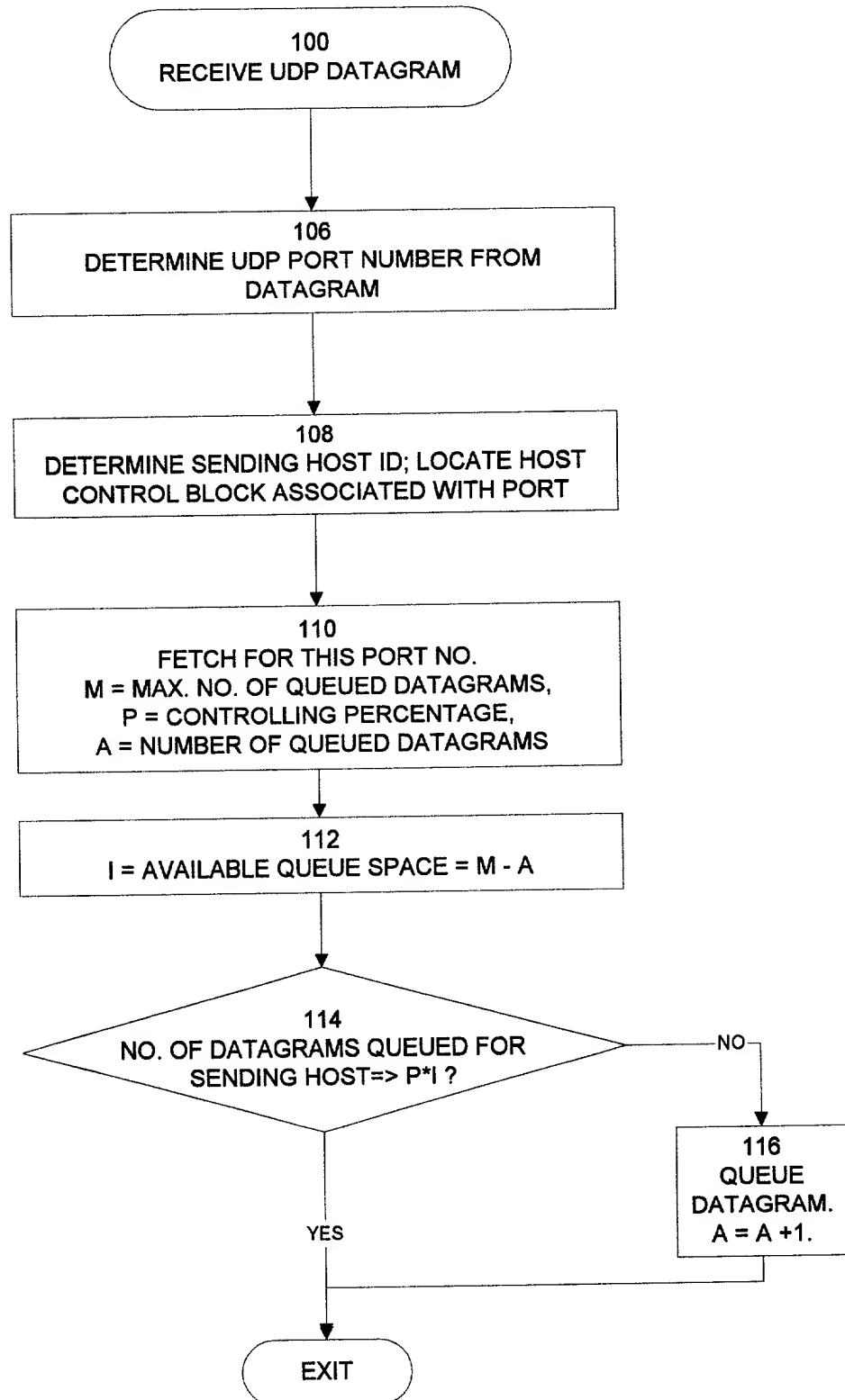
1 8. The carrier wave of claim 7 wherein the first code segment
2 further comprises:

3 a third code segment for calculating the prescribed
4 threshold by multiplying a percentage P by the number of

Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol

5 The invention prevents server overload and possible
server crippling due to a flooding of connectionless datagrams
caused by intentional attack or otherwise. In response to a
datagram from a host for a specified port, the number of
datagrams already queued to the port from the host is
10 determined. If this number exceeds a first threshold, the
datagram is discarded. In the preferred embodiment, the
threshold is determined by multiplying a percentage P by the
number of available queue slots remaining for the port.

FIG. 1



Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

TECHNIQUE OF DEFENDING AGAINST NETWORK FLOODING ATTACKS USING A CONNECTIONLESS PROTOCOL

the specification of which (check one)

☒

is attached hereto.

☐

was filed on _____ as Application Serial No. _____.

I hereby state that I have reviewed and understand the contents of the above- identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

Number

Country

Day/Month/Year

Priority Claimed

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Applications:

Serial No.

Filing Date

Status

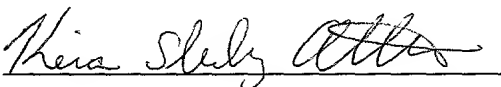
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

A.B. Clay, Reg. No. 32,121; G. M. Doudnikoff, Reg. No. 32,847; E. H. Duffield, Reg. No. 25,970;
J. W. Herndon, Reg. No. 27,901; J. S. Ray-Yarletts, Reg. No. 39,808; Gerald R. Woods, Reg. No. 24,144

Send all correspondence to: Jerry W. Herndon
IBM Corporation, Dept. T81/062
3039 Cornwallis Road
RTP, NC 27709
919-543-3754
FAX: 254-4330

(1) Inventor: **Kira Sterling Attwood**

Signature: 

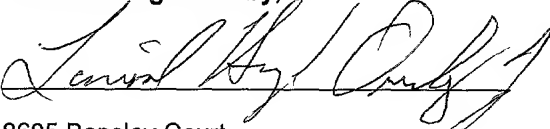
Date 2/11/2000

Residence: 1311 Pulpit Hill Road
Chapel Hill, North Carolina 27516

Citizenship: USA

Post Office
Address: Same

(2) Inventor: **Linwood Hugh Overby, Jr.**

Signature: 

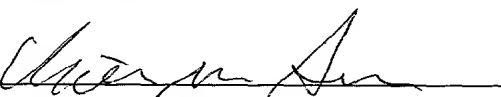
Date 2/11/2000

Residence: 8605 Bensley Court
Raleigh, North Carolina 27615

Citizenship: USA

Post Office
Address: Same

(3) Inventor: **Chien-En Sun**

Signature: 

Date 2/11/2000

Residence: 103 Chippoaks Drive
Chapel Hill, North Carolina 27514

Citizenship: USA

Post Office
Address: Same